A PHYSICAL SECURITY PRIMER FOR THE COMMUNITY

by dual_parallel
www.oldskoolphreak.com

"There are three simple principles to follow: keep people away, keep them out, and protect your plumbing."
Microsoft 5-Minute Security Advisor - Basic Physical Security

Unfortunately, physical security is not as simple as most IT-centric books and websites lead you to believe. Effective physical security is not a checklist. Effective physical security comes form a methodology that is applied system-wide (the idea of "system" discussed later). This article will present the foundation of a methodology that can be used to secure assets of any value, and then discuss a few specific technologies and how they are used (and misused) in the methodology.

Checklist? Methodology? Even more basic: What is physical security? First, what physical security is not. Physical security is not safety. For example, protecting your lab from accidental fire or storms and keeping harm from humans from said fire or storms is not security; that is safety. Security is the protection of assets from humans with malevolent intent, hereon called adversaries. Assets can be material objects, information or human life.

It was said that a system-wide view to physical security must be taken. Here, system does not mean a single computer or network, but the entire entity within which an asset resides. To the example of a hacker's lab, the computers within the room, within the house, the people that reside and have access, any security technology used, and any off-site security elements. That is a system. Every element interacts in some way.

Methodology

With security and system defined, it is time to describe the methodology. As stated, the object of physical security is to protect assets from adversaries. So defining what is to be protected and its value is the first step.

Let's take a hacker's computer containing dairy-fresh exploit code (ready for full disclosure). To the hacker, this is a high consequence asset, meaning that loss of the asset is unacceptable. An off-site backup would mitigate risk, but let's assume this is not possible. In this system, the greatest amount of resources will be spent securing this asset. Suppose this hacker is also an avid gamer and must protect a rare collection of 2D Saturn shooters. The games are important, but not as important as the noteriety from such a fantastic piece of code. Therefore, less resources will be allocated to protecting the Saturn discs. As can be plainly seen, defining what to protect and at what level is a first and important step.

As disturbing as this scenario may be, the hacker knows that a younger sibling covets the rare, round pieces of plastic. The desire for a classic, Japanese, vertically scrolling shooter transcends the notion of family - the young one is the adversary.